0. Identify the Attack Source

Create a Bash script to identify the IP address responsible for the most requests in a log file, which is likely the source of a Denial of Service (DoS) attack.

Functionality:

- Extract IP addresses from the log file.
- Count the occurrences of each IP address.
- Identify and print the IP address with the highest number of requests.
    - Log File : logs.txt

```
TIP: see which Ip had the most requests
```

```
┌──(oumaima㉿hbtn-lab)-
[…/web_application_security/0x0b_web_application_fast_incident_response]
└─$  ./0-attack_ip.sh logs.txt
**.***.**.**
```

```
grep -Eo '([0-9]{1,3}\.){3}[0-9]{1,3}' logs.txt | sort | uniq -c | sort -nr
| head -n 1 | awk '{print $2}'
```

Explanation of Each Step:

1. `grep -Eo '([0-9]{1,3}\.){3}[0-9]{1,3}' logs.txt`:
    - **Explanation of the Regex:**
        1. `[0-9]{1,3}`:
            - Matches a number with 1 to 3 digits (e.g., 1, 10, 255).
        2. `\.`:
            - Matches a literal period (`.`).
        3. `([0-9]{1,3}\.){3}`:
            - Matches three groups of 1–3 digits followed by a period (`1.1.1.`).
        4. `[0-9]{1,3}`:
            - Matches the final group of 1–3 digits (e.g., `1` in `1.1.1.1`).
        5. `-Eo`:

- `-E`: Enables extended regex for better readability.
- `-o`: Outputs only the matching part of the line.

2. **`sort`**:
   - Sorts the extracted IP addresses, which is necessary for the next step to count occurrences.
3. **`uniq -c`**:
   - Counts the number of times each unique IP address appears.
4. **`sort -nr`**:
   - Sorts the results numerically (`-n`) in reverse order (`-r`), putting the most frequent IP address at the top.
5. **`head -n 1`**:
   - Extracts the first line, which corresponds to the most frequently occurring IP address and its count.
6. **`awk '{print $2}'`**:
   - Prints the second field from the line, which is the IP address (the count is in the first field).

Example:

If `logs.txt` contains:

```
192.168.1.1
10.0.0.1
192.168.1.1
192.168.1.1
10.0.0.1
172.16.0.1
```

Running:

```
grep -Eo '([0-9]{1,3}\.){3}[0-9]{1,3}' logs.txt | sort | uniq -c | sort -nr | head -n 1 | awk '{print $2}'
```

Output:

```
192.168.1.1
```

This means `192.168.1.1` is the most frequently occurring IP address in `logs.txt`.